RESEARCH PLAN

ON

DESIGN OF SECURITY INTEGRATED ARCHITECTURE FOR BODY AREA NETWORKS

College of Engineering and Technology

Mody University of Science and Technology

SCHOLAR NAME: Aarti

ENROLLMENT NUMBER: 140302

SUPERVISOR: Prof. Partha Pratim Bhattacharya

DATE OF SUBMISSION:

INTRODUCTION

Body Ad hoc Network is real time network in which the network is defined as per individual. The specialized sensor nodes are defined in the network either on body or within body. These specialized sensor nodes are able to capture the particular human physiological signals and transit the captured information in associated form. For different organs, different kind of information can be captured by specific devices. Such as the brain information is captured as the EEG signal form and the heart information is captured as image form or the signal form. Such information includes image, signal and statistical information. A typical body area network incorporated with associated sensor devices and the connectivity to the outer world is shown here in figure 1.

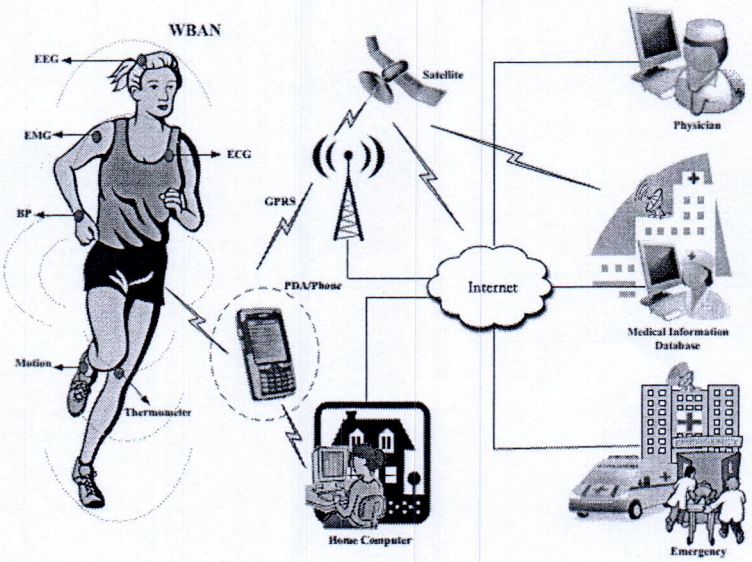


Figure.1. Standard Architecture of WBAN

Here figure is showing the standard body ad hoc network in which the individual BAN network and its connectivity to the outer world is shown. The figure here shows different sensors implanted or placed on human body to monitor different organs and various kinds of information is captured from the human being. Once the information is captured at the centralized device, it is able to communicate to the outer world. The centralized device can be a mobile handset or the specialized mobile device with internet enabled features. The single body area network can be of a patient, athlete, scientist or some individual working in extraordinary critical environment [1]. The controller PDA uses the mobile communication to capture this information.

This network form is not limited to single BAN or individual but it can include multiple individuals connected to share the information or define some comparative observation. The communication in this network form can be defined in different forms. In the simplest form, the intra-BAN communication is defined. In this form, the sensors capture the information and transmit it to the controller device. This real time communication can be single or multiple hop and respective to node criticality and communication form. The node sensitivity and patient disease also increases the criticality of intra-BAN communication. Another communication form defined in this network is inter-BAN communication. In this communication form, collected information from one WBAN can be transferred to other WBAN. This communication can be performed to generate a comparative observation or to provide the requirement specific communication. In most of the cases, the communication is here applied between the controllers. This inter-BAN communication

can be specific to the organ or the sensor or comparative. Such as to observe the walking capabilities of different racers, the relative captured information can be compared.

The inter-BAN communication can be performed in the same geographical area or can be unbounded. In case of unbounded geographical region, the communication can be performed through mobile communication. Because of this, the sensitive information can travel in the open public area. This kind of sensitive information can be captured by some intruder to capture the health history of an individual. To achieve the same and secure communication in this real environment, there is requirement of some security methods that can secure this communicating information.

This whole research work is captured surrounding these aspects of body area network. At the first level, the optimized clustered architecture will be formed to provide the effective inter-BAN and intra-BAN communication. This communication will be sensitive to the node type and captured signal analysis. Later on to provide the safe communication and to improve the communication reliability, the cryptography methods are applied. Different security forms are here suggested to provide the secure communication for inter-BAN and intra-BAN communication.

LITERATURE REVIEW

Author in [2] has proposed a Secure Authentication Model for Online Health Monitoring which makes use of the biological signals and the process of shared key establishment during the time of configuration. The key is exchanged once and that too only before the configuration of the network. The ECG and Blood platelet count of a person are used as the biological signals for the process of authentication which are stored initially in the warehouse at the time of the patient's registration. Here the communication occurs into two stages: Authentication Phase and Medical Data Transfer Phase. Their message digest is created and then encrypted with the shared key and sent to patient at the time of authentication which is then decrypted with the shared key and then matched with the sensed values of ECG and blood platelet count with the ones received. Medical data transfer occurs securely by encryption with the shared key. This scheme has low computational complexity and proves to better in terms of energy efficiency. The main problem that lies with this scheme is the compromise of the shared key. If the shared key gets known to the hacker then the entire Body Area Network is exposed to attacks.

In [3] the author has proposed an Authenticated Key Agreement and Cluster Head Selection for Wireless Body Area Networks. The communication here occurs in four phases: Keys Preloading Phase, Cluster Head Selection and Session Key establishment Phase, Cluster Head Rotation, Rekeying Phase. The selection of Cluster Head is based on the remaining energy and the Cluster Head is rotated from time to time in order to distribute the work among all nodes equally and save nodes from getting energy deprived by being Cluster Heads for a long time. Authentication is done by checking the Id of the sensors which wish to communicate with the Gateway. This scheme covers various security requirements ranging from Authentication, Confidentiality, Forward Secrecy, Backward Secrecy to Integrity. It has also proved to be better in terms of Communication overhead and memory requirements. The author has not worked on the freshness of keys. The communication process can be further optimized by using other parameters like sensing range, criticality.

In [4] Pham Thanh Hiep et. Al has come up with a cluster based two hop star topology to reduce the over concentration that leads to the deterioration of performance of the network. An optimization for method for access probability is proposed and the results show that cluster based topology proves to be better than the one hop topology.

In [5] KT Meena Abarna et. Al has proposed a Cluster based Failure Detection and Recovery Technique for Wireless Body Area Networks presenting a hierarchical architecture. Local nodes are made to communicate with the Cluster Heads and Cluster Heads with the Wireless Local Gateway. The Wireless Local Gateway in turn transmits the data to the Hospital Gateway. The local sensors collect fault related information and each node is assigned a priority to measure the fault tolerant level of individual nodes. Nodes with high priority are processed first. Node and Cluster Head level faulty node detection and recovery schemes have also been proposed. Results show that the proposed scheme is better in terms of reliability and fault tolerance. Here no work has been done on security else it would have been a complete security solution.

In [6] Sarah Irum has introduced a Hybrid Key management scheme for both Intra-WBAN and Inter-WBAN Communications. The proposed scheme uses preloaded keys as well as keys automatically generated from biometrics of the human body. Both inter and intra BAN communications provide the concept of rekeying and hence the data freshness is ensured. Four keys are used – administrative key, network key, basic keys and the key shared between Personal Server and Medical Server. These keys prevent the network from outsider attacks. Replay attacks are prevented by the use of timestamps. The proposed security scheme has proven better in terms of storage, communication, energy and security.

In [7] Aftab Ali has come up with a cluster-based security framework for both inter and intra WBAN communications. Keys are refreshed time to time and re-clustering is done time to time and also in the case when a Cluster Head leaves. The proposed scheme has proved to be better in terms of energy consumption and security. Here the concept of dynamic BAN has not been taken into consideration.

In [8] Prosanta Gope et. Al has explained the various security requirements in a WBAN modern healthcare system and has proposed a secure IoT-based healthcare system using Body Sensor Networks called the BSN-Care which can accomplish some of the security requirements. The BSN-Care server maintains an action table for each category of BSN data that it receives from the Local Processing Unit and as per the table it takes the required action on the data whether to take no action, inform family members, inform the local Physician or Inform Emergency when the value of particular BSN data reaches beyond a threshold value. The proposed scheme provides authentication, anonymity and resistance to replay attacks.

In [9] Zhaoyang Zhang has proposed a new cluster-based scheme for epidemic control. This scheme divides the populations into multiple clusters according to their social contact information and physical location. Then proposed control scheme is applied within the cluster or between the clusters. The drawback of this approach lies in the fact that not all people are willing to carry smartphones, few people are scared of sharing their personal health information with others due to absence of security, few people turn off their smartphones. This leads to missing information. Hence the approach cannot be successfully applied in such cases.

In [10] Vit Sipal et. Al has compared the propagation properties of WBANs for a fitness scenario, i.e., for subjects exercising squats and push-ups for three locations of the hub on the human body (waist, head, and foot). The best performance is achieved for hub location on the left temple and the worst performance by the waist-centric system, mainly due to the worst fading properties of such a channel. These results further provide a confirmation to that the previous works which show that the waist/hip may not be the most suitable location for hubs in future WBANs because other locations allow the use of directive antennas that reduce the impact of fading and improve the overall path-gain characteristics.

In [11] Shubhas Chandra has discussed the various wearable sensors that can be used for human activity monitoring, architecture of a human activity monitoring system and the various design challenges associated with them. Challenges in terms of security aspects require a detailed discussion and work can be done on it.

In [12] Preeti Chandrakar has proposed a secure and effective remote user authentication scheme based on RSA. It achieves mutual authentication and user anonymity properties. The proposed scheme is efficient in terms of communication and computation overhead. Work can be done to ensure integrity too.

OVERALL RESEARCH GAP

- Most of the research is focused on the work done on Single BAN.
- The dynamic nature of BAN has been ignored.
- Very less work has been done on security on inter BAN communication.
- Attack detection has been ignored where the concept of security has been applied.
- Clustering techniques can further be optimized by using parameters like coverage range, remaining energy.
- Heterogeneous nature of the sensor nodes has not been taken into consideration.
- Criticality of the nodes can be used for optimizing the data communication.

BACKGROUND AND SIGNIFICANCE

WBAN is the network that monitors an individual by placing the specific sensor devices on particular organs. These sensor devices are specific to the patient, disease or the organ criticality. Different type of communicating information and the placement of nodes also increases the communication challenge. When this captured information in transmitted in global world to get some remote feedback or the patient status analysis, the sensitive information is communication in open network. This kind of communication suffers from data leakage or intrusion as the health information is considered as the private information of an individual. Because of this there is the requirement of some secure method that will not affect the network efficiency.

In this work, a network of networks is defined for a region. Multiple-WBAN networks are composed with specific sensing responsibility. The optimized communication in individual WBAN and for overall network will be defined in this work. To provide the safe and reliable communication, cryptography method controlled by centralized controllers will be applied. The work will improve the network life and improve the packet communication.

Keywords: WBAN, Inter, Intra, Hierarchical, Clustered, Secure, Public Key, Private Key, Reliable, Architecture, Secure

OBJECTIVES OF THE PROPOSED RESEARCH WORK

The proposed research work will involve the following points:

1) The foremost objective of this research is to define optimized communication architecture for WBAN. The architecture will be able to provide the effective node selection and route formulation for both inter-BAN and intra-BAN communication. Effective methodologies will be defined based on real time characterization of network nodes and organ features.

2) The intra-BAN communication will be performed to optimize the individual WBAN communication. Here, the node features, organ criticality and the controller position will be defined effectively. Various measures will be applied for individual node selection to generate the all-to-center route. The sensor life improvement and resource utilization will be defined.

3) The clustered architecture will be formed, to provide the inter-WBAN communication. The aggregative controllers can communicate with each other to provide the information transition. The controller selection based multi-hop communication between these multiple WBAN will be performed.

4) To improve the communication reliability, the separate cryptography algorithms will be applied for both the inter-BAN and intra-BAN communication. The public key and private key authentication with encoded mechanism will be applied to improve the communication strength.

APPROACH / METHODOLOGY INTENDED TO BE ADOPTED

The proposed model will be defined specifically for a patient or an athlete in comparatively larger geographical region. Each of the individual will be defined with specific controller PDA device as well as the region specific main controller will be defined to capture the whole information. The architectural and security improvement will be applied over the network. To define the scenario and to improvement the work Matlab will be used as the simulator. Matlab is able to provide the effective method to generate the network effectively as well as allow the better graphical representation. The observed results can be defined in better way using Matlab features.

Objective 1: WBAN Architecture Generation with dedicated body devices and centralized PDA controller.

To provide this effective communication in this multiple-WBAN based wide network, an architectural formulation is required. The formation will be defined here respective to the specification of role and placement of individual body sensor as well as the controller. The network architecture will consider the following information while setting up the body sensor nodes

- Specific sensor for specific organ
- Specification of data communication based on organ
- Different energy backup for different sensor nodes
- Different criticality levels for different devices.
- Energy consumption while communicating or forwarding
- The placement of controller
- Role of controller

This objective will actually map the real time requirements including the device requirement, communication requirement and the individual requirement. The parameter selection and relative value definition will be done at this stage.

Objective 2: Perform Intra-WBAN communication and its optimization to deliver data to centralized controller

The intra-WBAN communication is considered more critical as the sensor devices are attached to the particular organ. The route formulation and intermediate node election is quite critical because of the device role and the organ criticality. The optimized single and multiple hop routing will be performed by observing the multiple parameters including

- Organ Criticality
- Remaining Node Energy of Battery
- Type of Communicating Information
- Coverage of Node
- Load on a node

By considering these parameters and characterizing the network and node features, the optimized intra-WBAN communication will be performed.

Objective 3: Perform Cluster Adaptive Aggregative Communication to optimize inter-WBAN Communication

The centralized PDA device will capture the aggregative data from individual sensors and transfer it to other WBAN controller or the main centralized controller. For this, the cluster formed inter-WBAN communication will be formed. The method includes the selection of controller for intermediate node and the relatively route formation will be done. This stage will take the decision respective to

- Collect the aggregative data on each centralized controller
- Identify the WBAN that can communicate directly to main controller
- Define the decision parameters for each controller in terms of coverage, load etc.
- Generate the multi-hop route to optimize the WBAN communication

Objective 4: Apply the security algorithm for both inter-WBAN and intra-WBAN communication using separate cryptography methods

The proposed work model will be able to improve the communication strength and reliability. For open space communication, the cryptography algorithm will be applied separately for inter-WBAN and intra-WBAN network.

- The cryptography algorithm for intra-WBAN will be light weight and public key inspired. The controller will distribute the keys and decryption will be applied at controller only. Here public key cryptography will be implied.
- The inter-WAN is having comparatively higher capability so that the private key encoded cryptography method will be applied at this stage. The main controller will generate and distribute the keys. The decryption can be performed by the individual controller as well as the main controller. During communication, the destination nodes will be specified for the decryption.

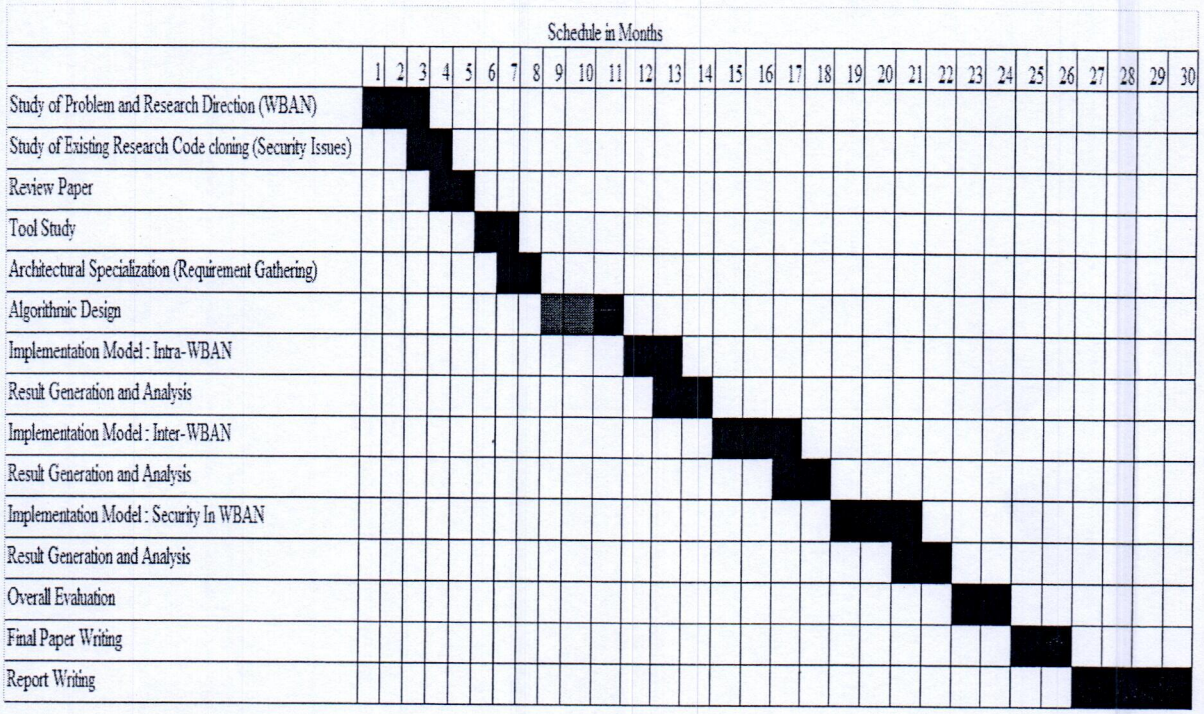
This work model will improve the network life, improve the network communication as well as will improve the communication security.

LIKELY OUTCOME/DELIVERABLES EXPECTED OUT OF THE PROPOSED RESEARCH WORK

In this work, an optimized secure network model is defined to provide the secure and effective WBAN communication. The inter-WBAN and intra-WBAN communication will be optimized by this work under different parameters. The work will be able to provide the outcome in following expected form

1) The first level optimization will be achieved at the individual node level. The individual nodes will be observed respective to particular sensor to generate the comparative observation. The criticality of organ or the node will be identified.
2) The comparative observation on different individuals or WBANs will be generated. The observation will be in terms of network life and the packet communication.
3) The strength of collective WBAN communication will be identified. The network life and the packet communication in the complete network will be observed.

GANTT CHART


Schedule in Months
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Study of Problem and Research Direction (WBAN)
Study of Existing Research Code cloning (Security Issues)
Review Paper
Tool Study
Architectural Specialization (Requirement Gathering)
Algorithmic Design
Implementation Model : Intra-WBAN
Result Generation and Analysis
Implementation Model : Inter-WBAN
Result Generation and Analysis
Implementation Model : Security In WBAN
Result Generation and Analysis
Overall Evaluation
Final Paper Writing
Report Writing

REFERENCES

[1] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith and Abbas Jamalipour " Wireless Body Area Networks: A Survey", IEEE Communications Survery and Tutorials" 16(3): 1658-1686, Jan 2014.

[2] Srivatsan Sridharan, Gorthy Ravi Kiran "Secure Authentication Model for Online Health Monitoring System", *In Proc. Of IEEE Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).* Pp. 1-5. July 2013.

[3] Jawaid Iqbal Nizamuddin, Noor ul Amin, Arid Iqbal Umar "Authenticated Key Agreement and Cluster Head Selection for Wireless Body Area Networks", *In Proc. Of IEEE 2nd National Conference on Information Assurance (NCIA).* pp.113-117, Dec 2013.

[4] Pham Than Hiep, Nguyen Huy Hoang "Maximizing Throughput of Cluster-Based WBAN with IEEE 802.15.6 CSMA/CA" International Journal of Multimedia and Ubiquitous Engineering, 2014 pp. 391-402.

[5] K.T. Meena Abarna and K. Venkatachalapthy,"Cluster Based Failure Detection and Recovery Technique for Wireless Body Area Networks", Research Journal of Applied Sciences, Energy and Technology, 2014, 7(17): 3458-3465.

[6] Sarah Irum, Aftab Ali, Farrukh Aslam Khan and Haider, "A Hybrid Security Mechanism for Intra-WBAN and Inter-WBAN Communication", International Journal of Distributed Sensor Networks, 9(8): 842608, Aug 2013.

[7] Aftab Ali, Farrukh Aslam Khan,"Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications" Journal on Wireless Communications and Networking, 2013.

[8] Prosanta Gope and Tzonelih Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network", IEEE Sensors Journal, Vol. 16. No. 5, March 2016.

[9] Zhaoyang Zhang, Honaggang Wang, Chonggang Wang and Hua Fang, "Cluster-Based Epidemic Control through Smartphone-Based Body Area Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 3, March 2016.

[10] Vit Sipal, Domenico Gaetano, Patrick McEvoy and MaxJ. Ammann "Impact of Hub Location on the Performance of Wireless Body Area Networks for Fitness Applications", IEEE Antennas and Wireless Propagation Letters , Vol.14, 2015.

[11] Subhas Chandra Mukhopadhyay "Wearable Sensors for Human Activity Monitoring: A Review", IEEE Sensors Journal, Vol. 15, No. 3, March 2015.

[12] Preeti Chandrakar and Hari Om "RSA Based Two-Factor Remote User Authentication Scheme with User Anonymity", *In Proc. Of Elsevier 4th International Conference on Eco-friendly Computing and Communication Systems*, vol. 70, pp. 318-324, 2015.